Breaking into Physical Red Teaming

Physical Red Teaming

Interested in breaking into physical red teaming? Whether you're new to the field, or a seasoned cyber penetration tester, this primer outlines a recommended path for expanding your skills, knowledge, and perspective to become a professional hacker, and expert physical red teamer. As always, please provide feedback and suggestions as we aim to update this guide regularly. Thanks for reading!

You can reach Ana, Shawn, and team by emailing info@pinerisk.com. We look forward to hearing from you and are excited to welcome you to the awesome field of physical red teaming!

Content

03 Breaking into Red Teaming: Phase 1

10 Resource: Red Team Job Descriptions

12 Breaking into Red Teaming: Phase 2

21 Breaking into Red Teaming: Phase 3

Breaking into Red Teaming: Phase 1

Follow these steps to gain the requisite skills and experience you need to be hired as a physical red teamer!

Twelve Steps to Becoming a Red Teamer

These posts include the core steps to help jumpstart your physical red teaming career. Regardless of the specific path to get into physical red teaming, these twelve foundational concepts are essential to being a well-rounded red teamer with the knowledge, skills, and context to make you an attractive candidate or consultant.

Phased Approach

Ready to become a physical red teamer? Diving into a new career path (or expanding a current one) is a massive undertaking. It is also difficult to know when you are ready to work in that field, and to know when you will have the competence and confidence to show for it. In other words, we all experience imposter syndrome, but we want to help get rid of yours.

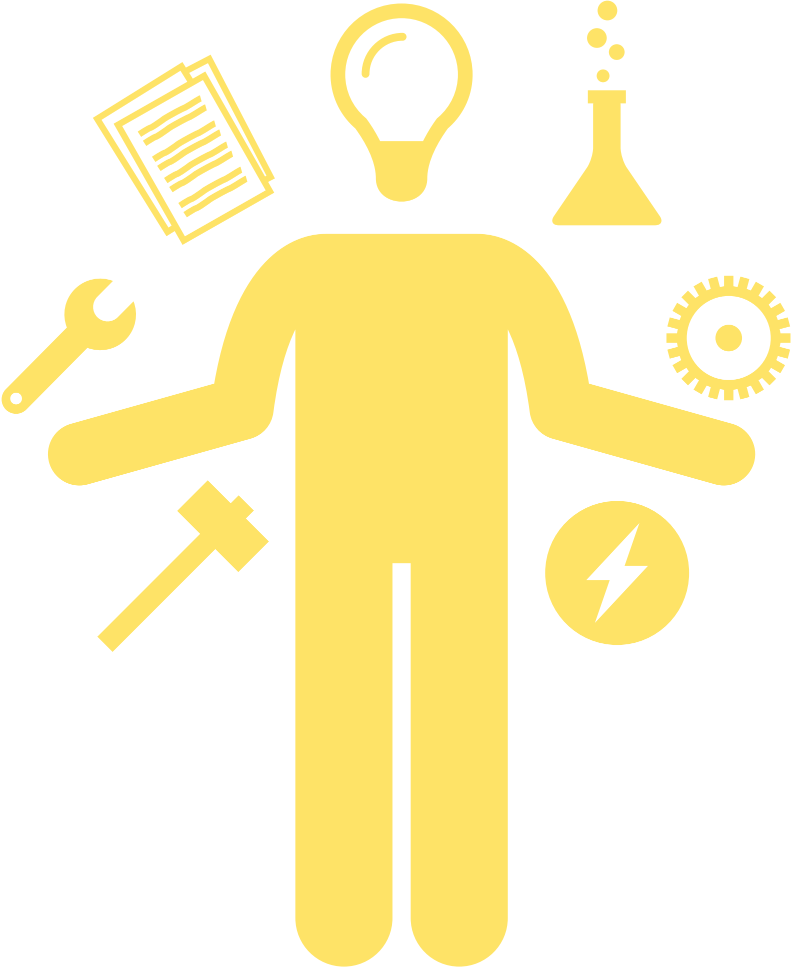
Our goal is to give you a roadmap that makes you a highly competent red teamer, and provides the clarity and structure needed to be confident in yourself, your skills, your knowledge, and your place in the security field as physical red teamer. As red teamers, we aim to provide you with a wide array of resources from different perspectives and professions. We have broken the training and ramp-up into three parts:

- **Phase 1: Fundamentals (this post):** What is red teaming, what types of red teams exist, where does red teaming fit into the wider security field, what is the difference between red teaming and penetration testing, and more. Understanding the profession, terminology, framing, and goals of a red team are essential to pursuing a career in the field. There are three steps:
    - Step 1: What is Red Teaming?
    - Step 2: Analytical Red Teaming
    - Step 3: Cyber Red Teaming

- **Phase 2: Technical Skills:** Every profession has specific skills that most practitioners are expected to maintain; physical red teaming is no different. From lock picking to OSINT, badge cloning to social engineering, we will cover the basic (and advanced) technical skills that physical red teamers are expected to have within the industry.
    - Step 4: Lockpicking
    - Step 5: Social Engineering
    - Step 6: OSINT
    - Step 7: Physical Access Control Systems (PACS): Badge Cloning and RFID Hacking
    - Step 8: Bypass Techniques

- **Phase 3: Employment Skills:** So, you understand the industry and have the skills to break into buildings. Now what? It's time to work on being an attractive employee or consultant. This entails effective communication around red teaming, report writing, partnerships with other types of red teams, knowledge of regulations and rules around red teaming, knowledge of security frameworks, ability to stay safe while red teaming, and an understanding of where physical red teaming fits into broader security picture of cyber, information, and physical security teams.

- Step 8: Red Teaming Ethics & Laws
  - 8a Red Teaming Gone Wrong
- Step 9: Red Team Risk Management: Staying Safe
- Step 10: Learning From the Real Baddies
- Step 11: Security Frameworks, Standards, and Regulations
- Step 12: Report Writing and Impactful Communication



Phase 1: Fundamentals

Timeline

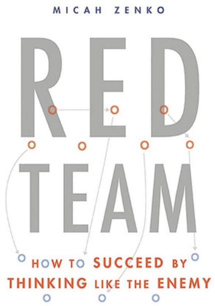
Phase 1 should take two months. If you rush the process, you will sacrifice depth of knowledge and the opportunity to take advantage of your new excitement about and dedication to physical red teaming. If you find yourself rushing, keep rushing! But do so intentionally. Take notes of key terms and concepts that interest you, and if you find yourself done early with the items listed in a specific phase, begin doing deeper research on those topics. Harness your curiosity instead of rushing through all three phases.

Note that while most red teamers have broad knowledge of the topic areas in all three phases, they will often also have incredible depth of knowledge in one or two specific subject matter areas. For example, if you find yourself suddenly passionate about combating groupthink, picking high-security padlocks, or OSINT-gathering on radical hate groups, then take time to research, pursue, and begin contributing to those red teaming specialties. Many areas of the physical red teaming profession are relatively new, and ripe for your contributions. By taking the time to conduct additional research, gain more skills, or publish tutorials online, you will contribute to the profession of physical red teaming, you will make yourself a better red teamer, and all the while you will become a more attractive job candidate or consultant.

Step 1: What is Red Teaming?

Before jumping into the skills and knowledge of the red teaming profession, you should be able to confidently describe to friends and family exactly what red teaming is, and it's not simply "picking locks and breaking into buildings." Red Teaming is a mindset, an organizational position, and a profession wrapped into one. It's applied in fields such as Analytical Red Teaming (sometimes called Applied Critical Thinking), Cybersecurity Red Teaming (most often just called Red Teaming), AI Red Teaming, and Physical Red Teaming. To speak to the wider field and approach of red teaming, you should read either:

- Red Team: How to Succeed By Thinking Like the Enemy - Micah Zenko
- Red Teaming: How Your Business Can Conquer the Competition by Challenging Everything - Bryce Hoffman



I recommend reading either of the two books, or both as they are excellent reads. Reading and internalizing stories, framing, and fundamentals of red teaming are essential if you are seriously contemplating a career in red teaming. Upon completion of your initial literary journey into red teaming, watch Deviant Ollam's "You're Probably Not Red Teaming... And Usually I'm Not Either" video:

You're Probably Not Red Teaming... And Usually I'm Not, Either [SANS ICS 2018]
Share
YOU'RE PROBABLY NOT RED TEAMING
...AND USUALLY I'M NOT, EITHER
SANS ICS 2018
Watch on YouTube

Step 2: Analytical Red Teaming

You have read at least one book about red teaming, mostly focused on Analytical Red Teaming (ART) and Applied Critical Thinking (ACT). Now it's time to dive deeper into that world to ensure you understand the concepts that you will apply to the physical space. Being knowledgeable about ART and skilled at ACT exercises are foundational requirements for being a good physical red teamer. They teach you how to detect and address the assumptions, missteps, or cognitive biases within the security space that you will be tasked with combatting. The most important thing a physical red teamer can offer is a mindset and perspective that differs from the mainstream security teams'. This is far more valuable than any specific skill.

This is foundational to being an effective physical red teamer. To begin on this journey, you should:

- Read: UFMCS Red Team Handbook V9.0 (Latest & Last Version Published)
    - You don't need to read the full thing! I recommend pages 1-82, and selecting 5-8 specific tools and techniques to familiarize yourself with. Be comfortable running a workshop where you use these techniques, and understand how they foster critical thinking, combat biases, and lead to better decisions.
    - My favorites: 1, 2, 4, Whole Group; 4 Ways of Seeing; Circle of Voices; Frame Audit; Mind Mapping; Key Assumption Check; Think, Write, Share; and of course, the all-time favorite: Pre-Mortem Analysis.

Step 3: Learn about Cyber Red Teaming

As a physical red teamer, you will frequently be collaborating with (and mistaken for) the cybersecurity red team. Learning the language and basic approach of cyber red teams is necessary to be a good partner, holistic security professional, and excellent physical red teamer. There are also a significant number of exploits that fall squarely between physical and cyber red teams.

For example, which team clones badges, pulls cameras off the wall and plugs in a laptop to see if they can access the corporate network, plants and uses keyloggers to capture passwords, conducts social engineering, and scans WiFi networks for weak passwords? There is no consensus on where the line between physical and cyber exists, and at many companies the line doesn't exist at all.

If you are starting from a non-technical background and want to learn about cybersecurity, hacking, and penetration testing, I recommend doing any two of the below items:

- Read through this site and this site and take notes on any terms, software, or acronyms you don't know in a document. Take some time to define and learn a bit about each of those terms as you come across them.
- Learn about 28 different attack types from MITRE's ATT&CK framework (two from each attack phase/column). Look up terms you don't know and gain general understanding of the language used, attack methodologies, and phases of attack.
- Complete a Udemy Cyber Security Course (Options: 1, 2, 3, 4, 5)
    - LinkedIn Learning also has cybersecurity courses, and most people can access for free with a library card.
- [Advanced] Obtain your Certified Ethical Hacker (CEH) Certification
- [Advanced] Obtain your CISSP Certification
- Read Trustwaves Blogs: Trustwave, SpiderLabs

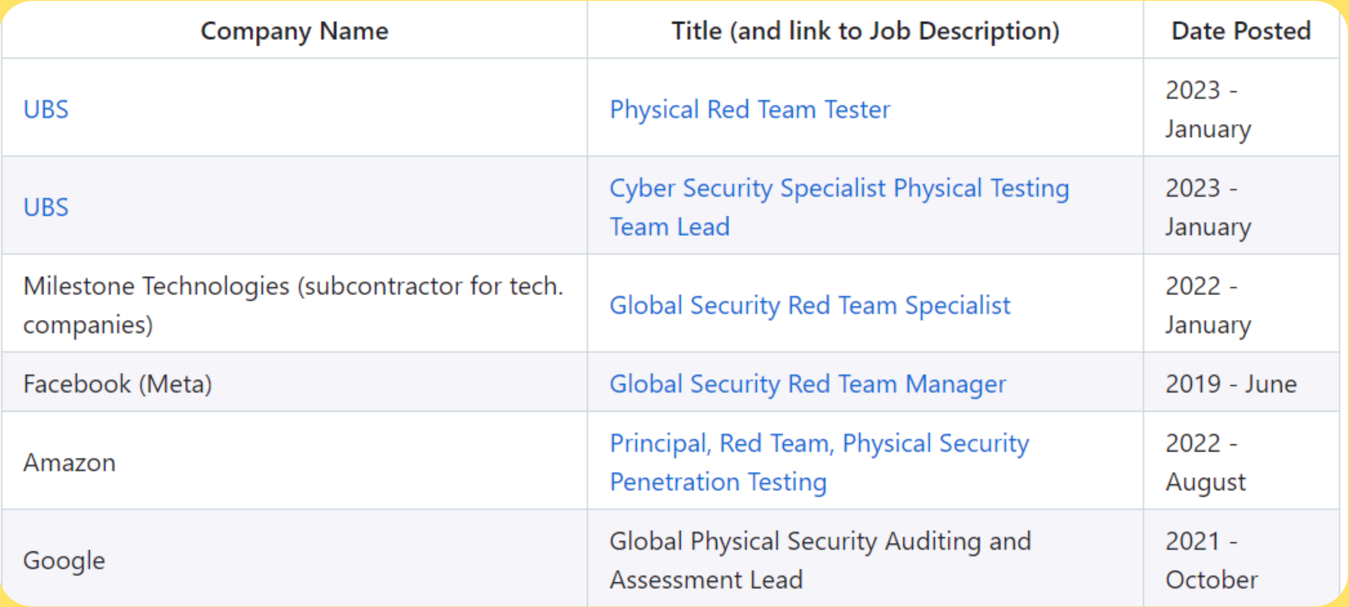
You don't need to become a hacker or programmer for this one, just gain a general understanding of the language, approach, and community of cyber red teamers that makes up the overwhelming majority of red teaming professionals today. Cyber red teaming is a larger and more mature field and profession than physical red teaming. As you learn about it, take notes and adopt their practices, templates, and approaches that you think can apply to physical red teaming.

Now let's get hands on! Phase 2 will focus on the skills that all physical red teamers should have.

Resource: Red Team Job Descriptions

Want a dream job? Check out these full time physical red team jobs from big tech and finance companies.

Over the last several years several companies have posted dedicated physical security red team positions: these are considered In-House Red Teams. Below are the ones I was able to capture and download:



Company Name	Title (and link to Job Description)	Date Posted
UBS	Physical Red Team Tester	2023 - January
UBS	Cyber Security Specialist Physical Testing Team Lead	2023 - January
Milestone Technologies (subcontractor for tech. companies)	Global Security Red Team Specialist	2022 - January
Facebook (Meta)	Global Security Red Team Manager	2019 - June
Amazon	Principal, Red Team, Physical Security Penetration Testing	2022 - August
Google	Global Physical Security Auditing and Assessment Lead	2021 - October

Please see the links to each job description below:

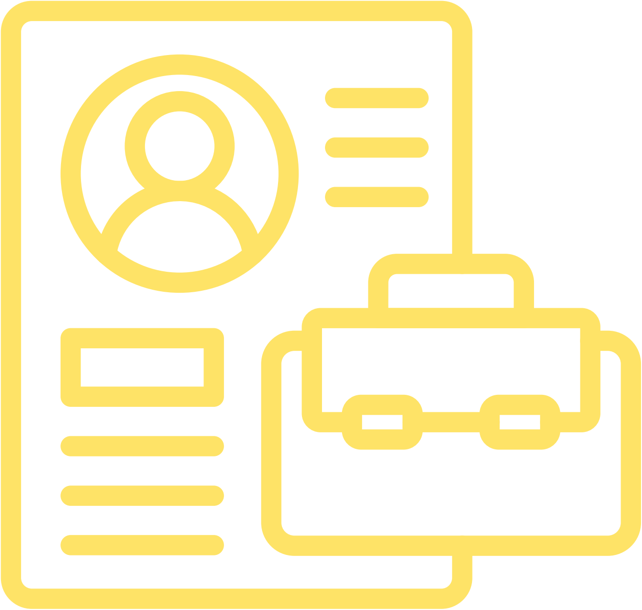
- UBS - Physical Red Team Tester
- UBS - Cyber Security Specialist Physical Testing Team Lead
- Milestone - Global Security Red Team Specialist
- Meta (Facebook) - Global Security Red Team Manager
- Amazon - Principal, Red Team, Physical Security Penetration Testing

We have captured these job descriptions and posts as a resource for the community.

The goal is to enable:

- Job Seekers to gain the skills and experience needed to be ready when the next in-house physical red team job becomes available.
- Security Managers to have examples of job descriptions that can be used to recruit red teamers.
- The Public to see examples of stand-alone in-house red team positions.

Physical red teaming as a profession is still in its professional infancy. With relatively few positions and even fewer formal resources, Locks & Leaks will continue to identify and publish the best industry resources to elevate the profession and allow the next generation to break into red teaming.



Breaking into Red Teaming: Phase 2

The skills and basic knowledge all physical red teamers should have.

Overview

This is the third post in a four-part series: Breaking into Physical Red Teaming. If you haven’t read **Phase 1**, it contains a description of timelines, an overview of our approach, and details on how we are working to prepare the next generation of physical red teamers.

You’re a red teamer so we know you like breaking the rules, but we suggest you start at the beginning for this one.

- Overview: Career Paths into Physical Red Teaming
- Overview of the Phases 1-3
- Phase 1: Foundational Knowledge

Timeline

This post focuses on the technical skills you should have as a physical red teamer. Phase 2 (steps 4 - 8) should take three months for you to complete. If you find yourself finishing early, we suggest that you do not proceed to Phase 3. Instead, find your favorite hands-on skill or an area you haven’t explored yet, and focus on that. Learn broader or deeper as it relates to hands-on red teaming skills. Boredom breeds creativity, and creativity is a red teamer’s best weapon. Practice honing your creativity in your free time. As a red teamer, it’s your most valuable intangible skill.

Step 4: Lockpicking

Become proficient at lockpicking. You don’t need to be an expert but aim to be intermediate. The skill itself will come in handy from time to time, but the real benefit comes in the fringes. By virtue of joining the lock picking community, you will find resources, perspectives, and industry voices that will shape you as a professional.

There are many ways to pursue lockpicking as a hobby and a career skill. I suggest you pick any two from the following list:

- Reddit/lockpicking: Try to make it to a greenbelt or beyond!
- Book: Practical Lock Picking
- Follow the Lockpicking Lawyer and watch at least 20 videos
- Take the Covert Methods of Entry (CMoE) Course (This is an expensive course - I recommend only doing it if your employer pays for it, or if you can easily afford it)
- New (Jan 2024) Locksport Book
- Get and complete one of these practice sets:
    - See-Through Option
    - Advanced Option: Note you are probably ready to progress after you complete Lock 5. If you complete Lock 6 that is a bonus.

Step 5: Social Engineering

Social engineering is a complex, controversial topic in the security awareness, penetration testing, and ethics spaces. It is also one of the essential skills for red teamers. You don't need to be extroverted or even good with people in order to become an effective social engineer. The most important thing is to know yourself, have self-awareness into how others see you, and exploit that to your advantage. For example, if you're a boisterous Type A, you can walk up and dive into an energetic conversation with security officers and they may forget to ask you how you even got into the building. If you are quieter, anxious, or timid, then find a social engineering role where you can use who you are to your advantage. For example, maybe you had an interview with the CEO and your wallet fell out of your pocket, but you can't email the CEO for fear of not getting the job. You also can't explain where it is exactly but can show the security officer. If you're nervous about social engineering, or interacting with people in general, then the security officer will see that….which is good. You told them a story where it makes sense that you feel nervous about asking. Your nervousness just went from being a weakness to an essential part of your story. Know yourself, and use that knowledge to your advantage.

If you are bad at lying, we have good news for you! The best lies to tell during social engineering are those closest to the truth. Often you can tell your target nearly the entire truth about where you need to get into, how your boss will be angry if you don't succeed, that you're new to the job, etc. All of these may be true, you just switched from being a red teamer to a janitor, but all the peripheral cover story data may still be true. Becoming an effective social engineer is intimidating for many; however, most people thrive in these roles once given the opportunity and a little bit of practice.

To learn both theories and tactics, start by reading a primer (IBM, Wikipedia, or article of your choice), watch a nice 2-minute example of effective social engineering, and then do two of the following:

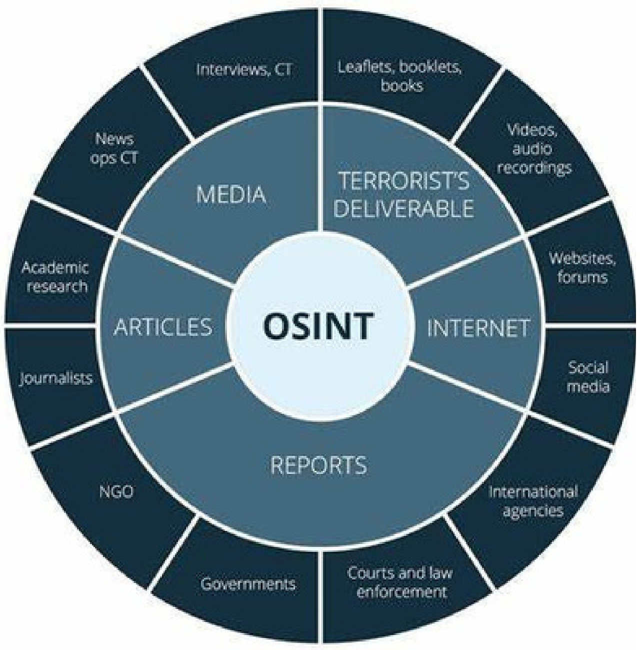
- Read a book from renowned hacker Kevin Mitnick. My favorite is The Art of Deception.

- Consider a book from Christopher Hadnagy:
  - Human Hacking: The Art of Social Engineering
  - Human Hacking: Win Friends & Influence People
  - NOTE: There are currently allegations against Hadnagy relating to his violation of the DEF CON conference code of conduct. You can read more about it yourself. I want readers aware of allegations and able to make their own decision.
- Attend Social Engineering (SE) Village at DEF CON: This is the single best educational experience you can have on your path to learning SE. You will watch live as individuals and groups conduct SE phone calls all over the country, and if you choose, you can participate and enter the booth to try it yourself.
- Watch one of the following Videos
  - Defcon 2019
  - CNN Report and Example of SE
  - Hacking Challenge at Def Con
- For an academic and economic view of Social Engineering, read ENISA's 2023 Threat Landscape Report. The introduction and overview are excellent, and the SE-specific section starts on page 71.
- Follow two of my favorite voices on Social Engineering and read several articles and/or watch their videos:
  - Rachel Tobac - CEO of Social Proof: LinkedIn, Twitter, Videos
  - Christina Lekati - Sr. Social Engineering Trainer & Consultant at Cyber Risk: LinkedIn, Medium

Bonus: I have heard Maxie Reynold's book The Art of the Attack is quite good, but have not read it myself. If you do, please let me know how you liked it, and whether you felt it prepared you for a career in physical red teaming.

Step 6: OSINT

Open-Source Intelligence (OSINT) has bloomed into a standalone profession in recent years, and the skills involved are relevant to nearly every cyber, physical, or information security professional. The knowledge of what information is generally and publicly available, and ability to find it, are a skill that can set you apart. OSINT has sprung into the mainstream over the past decade and moved from a skill many analysts had to a standalone profession with academic courses, schools, companies, and professionals all dedicated to only OSINT. In many ways, Locks & Leaks is using OSINT's professional emergence as a roadmap to learn from as we promote physical red teaming as a standalone profession.



To gain OSINT skills of a physical red teamer, we recommend to:

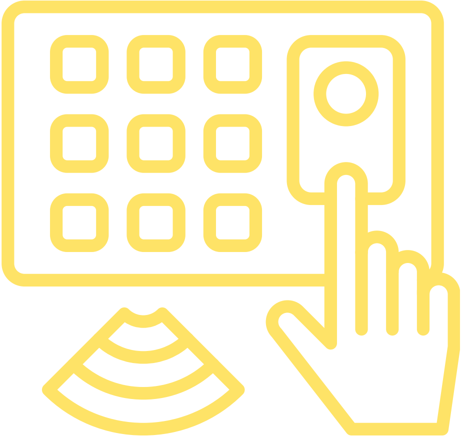
DO THIS: Michael Bazzell is a household name for OSINT. He has the original, and best, books around OSINT and privacy. I highly recommend getting his latest book from 2023, reading it in full, and practicing with the tools and resources he covers. Do this, and you will be ahead of 90% of security and even many OSINT professionals.

To gain OSINT skills of a physical red teamer, we recommend to:

DO THIS: Michael Bazzell is a household name for OSINT. He has the original, and best, books around OSINT and privacy. I highly recommend getting his latest book from 2023, reading it in full, and practicing with the tools and resources he covers. Do this, and you will be ahead of 90% of security and even many OSINT professionals.

DO TWO OF THESE:

- Spend a few hours clicking through, researching, and bookmarking key resources from SANS guide on getting into OSINT. Note the age of some of the recommendations. Anything that has not been updated in two or more years is likely out of date. You can do this on SANS' website, or any of the below guides:
  - Job-focused starter's guide to OSINT: OSINT-Jobs
  - The first and best to institutionalize OSINT: Bellingcat's Guide
  - Resources for practioners that want to go deeper: The Sleuth Sheet
  - If you want to build your street cred with OSINT, here are great recommendations: Secjuice
  - Consider a GOSI Certification.
  - Become familiar with the OSINT Framework.
- Read Rae Baker's Book: Deep Dive - Exploring the Real-world Value of Open Source Intelligence
- Get involved in an OSINT Capture The Flag (CTF) Community, Team, or Group. Solve a few CTFs, get stumped, learn new skills, and try again. Here are some great resources:
  - List of 15 Practice CTFs
  - Wide Array of Available CTFs & CTF Communities
  - Trace Labs: CTFs for Good



Step 7: PACS Attacks

Physical Access Control Systems (PACS) are the badges, badge readers, door control panels, badging software, and other hardware and software involved in access control. There are many attacks on these types of physical security systems, and as a physical red teamer, you will be expected to be knowledgeable about them.

The primary attack types you should know about:

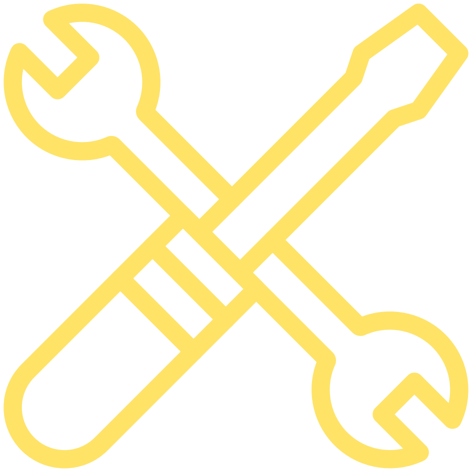
- Man-in-the-Middle: ESPKeys are the best example of this. This is a type of eavesdropping attack.
- Credential Cloning: Badge Cloning Attacks
- DDOS Attacks: Denial of Service for Badge Readers
- Tampering: Physically manipulating PACS hardware (e.g., shorting a circuit, implanting a device, etc.)
- Relay Attacks: Involve capturing the signal from a legitimate access device (like a key fob or card) and transmitting it to the reader from a distance, effectively tricking the system into thinking the attacker is the legitimate user. This type of attack is particularly effective against systems that do not employ proper distance bounding protocols.
- Side Channel Attack: Although rare, it's not out of the picture when it comes to hacking PACS.

There are occasionally excellent conference talks (con talks) about these types of attacks, but they have become rarer as PACS companies become aggressive in targeting researchers who publicize their vulnerabilities. A few of my recommendations:

- Watch One of these Two con talks by Babak Javadi & team.
    - Follow Babak on LinkedIn
- Take some time to research this yourself; there are a slew of resources out there focusing on many technologies, vendors, card types, and protocols involved in physical access control systems.

Step 8: Bypass Techniques

Here's the fun one! Bypass techniques offer a range of ways to circumvent security measures - typically doors and latches. Most physical red teamers should be proficient at all of these, good at 50%, and great at 25%. Having a team with diverse skills to tackle whatever measures you face will be important. Become comfortable with how these tools feel in your hand when attacking different locks, doors, and latches. Watch videos, set Google Alerts, and keep an eye on the latest exploits and add-ons when it comes to the ever-expanding market of bypass techniques.



Here are some of the most common:

- Under the Door Tool (click the “Video” tab to see it in use)
- Locks/Keys (see Step 4 above)
  - Picking
  - Bumping
  - Impressioning
  - Decoding
- Thumb-Turn Tools (product)
- Shims (Video | Cylinder Shim | Steel Shim)
- Hinge-Pin Removal (Video | Purchase)
- Latch Loiding (Video | Tools)
- Double Door Tool - DDT (Video | Tool)
- Shimming (Video | Tool)
- Over the Door Film (Video | Tool)
- Request to Exit (REX) Trigger (Whisky | Compressed Air | Hand Warmer | Tools)
- Elevator Hacking (Video)
- Many More: Find videos of your favorite bypass techniques on YouTube and follow their channels. Find those presenting new exploits at cons and follow their social media or set up Google Alerts for them. In general, red teamers will be expected to stay appraised on the latest and greatest in these techniques.

Note: Inevitably in your career you will be stumped during an assessment (or at home practicing) and you will develop a new technique, tool, or both. Share your innovations! Tag your favorite red teamers, present your hacks at conferences, or publish a video/tutorial. The red team industry moves forward by sharing innovation with the community, and the entire security industry moves forward by red teamers pressuring them to improve and fix vulnerabilities before adversaries exploit them.

Conclusion

Don’t let anyone gatekeep red teaming for you. No one is expected to be perfect, or even good, at all of the above techniques. Learn and practice as you go. If you don’t have a job that involves red teaming, build an at-home lab to practice bypass techniques, or practice on various buildings and lock types where you have connections (get permission!). Spend time to get both familiar and adequate at each of the technical skills. Most of red team learning is on the job or in the classroom. If you’re just breaking into the red teaming field, learning the basics of each skillset above should take at least 3 months. I would suggest 6 months if you really want to familiarize yourself, practice, and grow. Whatever timeframe you set for yourself, you now have the context (Phase 1) and the skills (Phase 2) to become a physical red teamer. Now it’s time for the final phase: Employability.

What makes you an attractive, well-rounded red team candidate? What instantly positions you to be a physical red team leader? We’ll discuss the mindset and skills needed in our next post!

Breaking into Red Teaming: Phase 3

The key(s) to being a recognized and sought-after red team operator.

Overview

This is the fourth and last part in our four-part series: Breaking into Physical Red Teaming. If you haven't read Phase 1, it contains a description of timelines, an overview of our approach, and details on how we are working to prepare the next generation of physical red teamers.

You're a red teamer so we know you like breaking the rules, but we suggest you start at the beginning for this one.

- Overview: Career Paths into Physical Red Teaming
- Overview of the Phases 1-3
- Phase 1: Foundational Knowledge
- Phase 2: Skillz
- Phase 3: The Professional Red Teamer [This Article]

Timeline

This post focuses on the professional, employability, and soft skills you should have as a physical red teamer. Phase 3 (steps 8 - 12) should take two months for you to complete. If you finish early, then pause and practice the soft-skills that are your biggest gaps. Whether it's public speaking, knowledge of Advanced Persistent Threats (APTs), or understanding industry frameworks, take the time to become a well-rounded red teamer with these skills.

Bored? Good. These are the least-exciting skills in the toolbox of a top-notch physical red teamer, and they're also the most important. The fact that these are less exciting than breaking-and-entering skills is exactly what makes them rare among operators, and is what will set you apart from the rest of your peers. You have gotten good at hacking locks and badges, now focus on hacking the workplace by making yourself more employable as a red teamer.

Step 8: Red Teaming Ethics & Laws

Ethics: Your job is to now act unethically, ethically. In other words, how do you pretend to be someone acting unethically while still being ethical? They call red teamers "ethical hackers" for a reason. Same tactics, opposite motivation from the bad guys. Being creative, having strict ethics, and never losing sight of your ultimate goal are your best assets as you tackle the difficult task of being ethical adversaries.

Here are some steps to take:

- Watch "Red Team Ethics" by Roy Iversen and Tarah Wheeler.

Red Team Ethics - Roy Iversen & Tarah Wheeler talk ShmooCon 2020

Do Unto Others:
A Red Team Ethical Framework for
Offensive Rule f Engagement

Tarah Wheeler and Roy Iversen

Shmoocon 2020
January 31, 2020

- Review HackTheBox's Ethics in Ethical Hacking Explainer.

- Take time to think about, research, and write out responses to each of the scenarios listed in this post. Don't do more than one a day to give yourself time to consider options. Ask friends, co-workers, and security professionals what their opinion is and spend time writing answers from various perspectives. For example, write how you would feel about a social engineering scenario as the red teamer, as the security leader, as the victim of social engineering, and as the company leader. There's no right answer, but I'll give you two hints: 1) You should always be asking the question "Is this worth it?", and 2) Most ethical conundrums can be navigated or avoided by simply being creative. I suggest doing one or two of these per week, while also honing and improving your skills. The insight you gain from previous ethical questions, plus legal and ethical readings, in combination with the writing improvement, will all result in significantly increased and improved responses as you progress. Not to worry, because the questions get harder as well. You can view the scenarios HERE.

- Draft your own Code of Ethics as a red teamer. Google cybersecurity code of ethics and similar search terms to do research, and then draft your own list of principles, ethics, and values that you will live by as a red teamer.
    - Note: Moving forward you should have flexibility around this Code of Ethics. Not in whether you follow it; you should always adhere to the ethics and principles you lay out for yourself. You should have an open mind and willingness to update your personal Code of Ethics as you grow as a red teamer, as you change jobs, as the industry you work in changes, etc. A willingness to grow, learn, and adapt, combined with a strong Code of Ethics will take you very far as a red teamer.

Red Teams & Laws

This is an essential area for professional red teamers to be well-versed in. Spend time researching your local laws, learning about red teams gone wrong, and thinking through what steps you will take to stay on the right side of the law.

Here is our recommended reading:

- Laws that Red Teamers Should Know
- De-Risking the Red Team: Introduction
- De-Risking the Red Team: Legal Implications
- Watch the Coalfire Debrief with Brian Krebs after the Iowa arrests.
- Review the Updates
- Review the Federal Lawsuit filed by the Coalfire testers against Dallas County. (Click the “Download PDF” button to view documents).
- Review, in detail, this After-Action Report.

Bonus: There was a case where a pen tester was hiding in a parking garage somewhere in Europe, waiting to break into a building. A woman left the building and got very scared by the random tester hiding in the garage near her car. Although inadvertent, this is a notable case that caused both real-world harm to the company’s employee, and reputational damage to the company since it made the news. With that said, we can’t find the article we read about this event. If anyone finds it, please add the URL to this article in the comments and we will give you a shout-out in the next article we publish!

Step 9: Red Team Risk Management

Now that we reviewed the worst-case scenarios, let’s talk about how to avoid them. There are many steps to take during the steps of a red team engagement. From scoping to planning, surveillance to infiltration, here are some key steps to take at each step. As a current or aspiring physical red teamer, you should familiarize yourself with each area below and note that these are the bare minimum steps a professional red team should take prior to an engagement.

Scoping:

- Ensure you identify the exact locations being tested, and the relationship between the organization hiring you, the building owner, building management, security providers, and more.
- Obtain leases or other legal agreements that may shed light on the permissibility and constraints relating to what you can (and cannot) test.

The Proposal:

Whether you are an in-house red team or a consultant, you should be drafting a proposal or similar plan that outlines the specific goals, tactics, approach, threat model, communications plan, safety plan, and more. Take an hour (or more) to practice documenting the various safety measures for the below scenario.

> *You are a consultant hired to conduct a red team of an oil refinery. The client has asked you to conduct the test during the day, during operations, and during business hours. They encourage you to test their physical measures, technology, and personnel. You assemble a team of six experienced testers with a wide array of skills to complete the job. The Director of Corporate Security that oversees security for the offices and various refineries has hired you. They called the local security manager and let them know a test would occur in the next month. No one else on-site knows about the test.*

Complete the following sections for this hypothetical proposal:

- Letter of Authorization: Who drafts it, who signs it, whose contact information is included, and what letterhead is it on?
- Notifications: Do you notify law enforcement (LE)? Do you need additional individuals on site to be informed of the test beforehand? Develop a notifications plan.
- Communications: Develop a communications plan internally for the team, and externally for the client as the test progresses. How, where, and how often do you communicate with each party? Employ your best business continuity planning; develop plans B and C to ensure you have ways to reach all critical players.
- STOPOP: What are the triggers for Stopping Operations (STOPOP)? Is it when goals are met, or law enforcement is called, when the first individual is identified by security, etc.?
- Safety Plan: Develop a safety plan, including listing potential hazards/risks, and Risk Mitigation Measures for each of the areas (and any others you can think of):
    - Legal/Compliance Risks: Is there risk of running afoul of laws? If you are trying to lift (pickpocket) a badge off an unsuspecting employee, is there a chance that they view unwanted touch as assault? Are there any regulatory bodies or concerns relevant to this type of client that you need to adhere to? (Hint: there are.)
    - Privacy (Laws & Ethics) Risks: Will you be accessing sensitive information on individuals or corporations? How do you ensure you are on the right side of privacy laws, and beyond that, how do you ensure you are ethical about your approach to gathering/leveraging sensitive information as part of this operation.
    - Law Enforcement Risks: What is the likelihood that LE will become involved, and what is the plan to prevent this from happening, detect it in case someone does call, and react quickly to cancel or de-escalate any situation involving law enforcement?

  - Escalation Risks: In what ways could this scenario escalate? Could the refinery shut down operations (resulting in business loss), could their GSOC notify company leadership of an active emergency, or are there other notable ways the situation could escalate outside the control of the red team?
  - Weapons/Firearms Risks: Are there firearms or other weapons on-site? Could employees, bystanders, or security be carrying weapons? In what scenarios could they draw or use weapons, and how do we mitigate against this risk?
  - Environmental Health & Safety (EHS): Are there chemicals on-site? Are there any lasers, high-temperature, dangerous equipment, heights, or other potentially dangerous equipment or EHS scenarios to plan for?

Safety Brief: Prior to going into the field (even for surveillance), the entire field and oversight team should sit down and do a safety brief. The discussion should cover the operation’s goals, scope, communication, escalation procedures, key risks, risk mitigation measures, and when to STOPOP. Each member of the team should have an opportunity to ask questions, challenge any assumptions in the planning process, and voice concerns.

Prior to going out into the field, you should always do a safety brief with all involved parties to cover the ground rules, communication plan, and risk mitigation efforts. It may seem like overkill, let me tell you from experience that every scenario I mentioned has come up more than once in real-world assessments that I have done or led. Having worked through the risk mitigation plans ahead of time makes it easy to be decisive, safe, and effective. It protects you in the field, in the boardroom, and in the courtroom. Taking the time to proactively identify risks showcases to clients and your team the professional rigor that you put into each assessment. Take the time to develop robust safety plans prior to entering the field. All in, this should be a two-to-five-page document, using tables and bullet points to organize data into easily digestible content. It can be internal to the team or shared with the client as an assumption-check to ensure you proactively identified key risks.

Lessons Learned: Finally, all red teamers should keep their own Lessons Learned. Following an assessment, there should be a debrief to cover how the operation unfolded itself, and to discuss any lessons learned and areas where improvements can be made. By capturing these lessons learned, and reviewing them before the next assessment, you will continue to manage your risk, improve your capabilities, and hone your craft as a red team.

Step 10: Learning From the Real Baddies

Take one month to digest as many movies, news reports, YouTube videos, books, and other media about stories of heists, cybercrime, organized crime, espionage, and other crafty criminals as possible.

Resources:

- Podcasts
  - Heist Podcast
  - Last Seen
  - The Lazarus Heist
- Movies & Shows
  - Heat (Movie) - High-stakes heists
  - The Americans (TV Series) - Espionage, deep cover, and operational security.
  - The Italian Job (Movie) - High-stakes complex heist.
  - Argo (Movie) - Disguises, espionage, and psychology of pretending to be someone that you are not.
- Articles, News, and More
  - Set Google Alerts for your topics of interest and read (at least) the headlines each day.
  - Set up Google Alerts relating to your industry to track attacks against similar companies.
  - Read Verizon’s DBIR

    - Follow corporate reporting on Advanced Persistent Threats (APTs) and read the latest reports:
        - Google Threat Analysis Group (TAG)
        - Microsoft Intelligence Reports
        - Meta's Threat Disruptions
        - 2430 - The Red Report
- YouTube Videos: Find relevant topics and review articles relating to various breaches and approaches. From Urban Explorers to Protest Groups to breaking into the power grid, spend some time on YouTube finding relevant heists, breaches, and content to learn from. These also come in handy if you are in a meeting and need a quick example of real-world scenarios of breaches to quickly demonstrate.

Write About the Following Topics: Take time to write a page or more of content, answering each of the following questions.

1. What is your favorite heist in history? Why?
2. What are your favorite examples of excellent OpSec? What are a few examples of horrible real-world OpSec that resulted in arrests or worse?
3. Which of the threat actors in the corporate threat reporting do you think have physical capabilities? How might they show up and use in-person attacks to aid in their mission?
4. What trends in recent news stories, breaches, and heists have you noticed? How will that information aid you as a red teamer?

Step 11: Security Frameworks, Standards, and Regulations

This one is admittedly the least sexy, but often one of the most important facets of security assessment programs. Ultimately, audit teams assess against some sort of standard, framework, regulation, or specific set of requirements, while red teams assess a program against its performance when faced with real-world adversarial tactics. In other words, every assessment needs something to be compared against in order to be useful; otherwise, you are simply making observations about a security measure.

For example, without anything to compare against, you may state “The security guard was standing in the corner of the lobby, looking at their phone”. Is this allowed or expected behavior, or does this violate a written policy, goal, or procedure of that guard? An auditor, who is assessing against the Federal Risk Management Process (RMP) may note that the security guard should be visible (check) and monitoring ingress/egress (unlikely to receive a ‘passing’ grade on this one). A red teamer will compare the expected performance of a security officer (they deter, detect, and prevent unauthorized entry) to the actual performance (they don’t notice the tailgating alarm as you tailgate into the building). All said, knowing what you are assessing against is a very powerful tool for any red teamer.

Additionally, the ability to show a client or internal team that they are not meeting a requirement laid out by an industry standard, framework, or regulation can be a powerful motivator to correct deficiencies. You may be asked “well why do we have to fix this, no one would break in the way you did!”. Instead of pointing to your theoretical threat model, you can point to standards put out by the federal government, industry groups, and other entities that establish an expectation of security working in a certain way. Once you establish the broader existing norms and best practices, you can then detail your threat model, and finally discuss the performance of each layer of security against the norms and against the threat scenarios you tested against. That sends a much more poignant - and targeted - message to the blue team responsible for managing the organization’s defenses.

For those interested in red teaming, we highly recommend familiarizing yourself with these frameworks. You don’t need to memorize them, or even read them fully. Instead, download and skim each one. Understand what information is available and store it in a library you can use on your next (or first) assessment. We also recommend picking a few controls and threats (e. g., “security officer in lobby”, “camera coverage”, and “location of door hinges”) and look for any references to those controls within the standards. This familiarizes you with how to look for relevant material and the level of specificity each standard contains. Some will include specific details about the type and location of hinges, while others may simply state it must be difficult to remove the door from the outside. Understanding where and how to find this information is critical for a professional physical red teamer.

Standard to Review:

- Adobe Common Controls Framework
- NIST 800-53
- DHS: Risk Management Process for Federal Facilities
- Federal Facility Security Levels: One, Two, Three, Four, and Five
- U.S. Army: Security Guard Standards
- There are many more. Use Google, ChatGPT, or your favorite research tools to find the relevant standards, guidelines, and regulations that cover your topic areas. A red teamer well-versed in what the industry norms are is a red teamer that can articulate the impact of their assessments, avoid missing common tests, and help their organization remain ahead of the competition.

Step 12: Report Writing and Impactful Communication

Most employers and clients will want both written final reports, and a presentation of findings. The best red teamers are able to take complex, convoluted, and contentious topics and present them clearly, concisely, and confidently. Whether you are linking a series of vulnerabilities together to make an impactful attack chain or presenting a critical finding to a high-ranking and non-technical executive, effective communication is essential for professional red teamers.

here are many ways to improve these skills, but nothing beats practice. Whether you're new to red teaming, or aiming to level up your skillset, this is one of the most important focus areas. Take one final month of focused time to practice and improve your capabilities. Focus on being able to answer key questions to various audiences.

THere is a copy of our red team writing practice sheet. Edit the questions and audiences as needed to meet your career goals or match your current position. Take a stab and answering these questions now. Ask for feedback from various parties and work to improve the answers.

As you work through the practice sheet, we recommend taking a few courses and watching a few of our favorite videos about writing an impactful communication:

- LinkedIn Learning (Use your local library card for free access!)
  - Ninja Writing - Excellent course that teaches you how to write with impact. Spend time on this and try all the practice modules.
  - Leading with Vision - The easiest way to motivate people to action is through a compelling vision of what the future could look like if they do (or don't) act in a certain way. This course gets you excellent free online access.
- Podcasts
  - Think Fast, Talk Smart - Apple, Spotify (Listen to at least 6 episodes)
  - Darknet Diaries - Listen to at least 4 episodes. Focus on how Jack tells stories and brings the reader along. Find episodes relevant to your line of work and physical red teaming.
- Practice
  - Practice writing and presenting every single day. This may be as simple as asking ChatGPT to asking you two random questions relating to physical red teaming, and then you verbally respond to one (3-5 minutes) and write out the second. In this scenario, you should record your verbal response, watch it after, and write down how you'd like to improve for the following day.
  - Whatever you do to practice, just make sure you are consistent, repetitive, creative, and give yourself an opportunity to learn and improve as you go. Try to explain to non-technical friends or peers about concepts of red teaming in 90 seconds or less. One of the hardest parts of red teaming is trimming down complex and detailed content to simple, compelling, and clear statements that meet your audience where they are.
  - Find a way to practice and let us know what worked (and didn't work) for you!

Bonus Step 13: Lessons Learned

This is a red team special: take some time after you have completed all twelve steps to write about what lessons you learned. From how you learn best, to whether you trust strangers on the internet to lay out lesson plans for you, to which specific steps were most interesting, all the way to how you would improve this 12-step plan, take some time to capture the lessons you learned throughout this process. If you're willing, send it to us when you're done! We're always trying to improve our material, help our community, and learn from our peers. That's you now!

You're Done!

Congratulations, you did it! If you went through each of these steps and followed our painstaking roadmap (or improved upon it), then please send us a message or make a comment below! The physical red team community is small, and we (and our peer companies) are often looking for physical red teamers to join as consultants or employees. Drop us a line, let us how the process was, and we'll make sure to add you to our red team rolodex.

LOCKS & LEAKS

08 / 09 / 2024
hlocksandleaks.substack.com/